



Finanz Colloquium
Heidelberg

Banken-Times **SPEZIAL**

IT / ORGA / NEUE MEDIEN

März & April 2014

Finanz Colloquium Heidelberg

eMail: info@fc-heidelberg.de

Web: www.fc-heidelberg.de

In Zusammenarbeit mit:



Roland Hein
- Geschäftsführer -

bit Informatik GmbH

WIP - Der Wissenschaftspark Trier
Am Wissenschaftspark 32
54296 Trier

Tel.: +49 651 966 29-112

Fax: +49 651 966 29-100

eMail: roland.hein@bit-informatik.de

Web: www.bit-Informatik.de

Sehr geehrte Damen und Herren,

unser Newsletter enthält in dieser Ausgabe Beiträge zu **Risikoanalysen beim Outsourcing** sowie **Datenschutzrisiken bei Facebook-Fanpages von Banken**.

Die Inhalte haben wir zusammen mit unserem [Kooperationspartner bit Informatik](#) gestaltet. bit Informatik bietet Standardsoftware zur Umsetzung von gesetzlichen und bankfachlichen Anforderungen an, Schwerpunkte liegen in der Umsetzung von Programmeinsatzverfahren sowie der Vergabe und Kontrolle von IT-Berechtigungen.

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de. Wenn Sie einen eigenen Gastbeitrag verfassen möchten, freuen wir uns ebenfalls über Ihre Nachricht.

Mit besten Grüßen aus Trier und Heidelberg,

Roland Hein, Geschäftsführer, bit Informatik GmbH

Thomas Göhrig, Geschäftsführer, Finanz Colloquium Heidelberg

Risikoanalysen beim Outsourcing

In den letzten Jahren haben Kreditinstitute damit begonnen, Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen auszulagern (Stichwort Outsourcing), die in der Vergangenheit von den Instituten selbst erbracht wurden. Die Gründe für diese Maßnahme sind sehr unterschiedlich. Zum einen bieten Unternehmen im Verbund hierzu die Dienstleistungen zu einem sehr guten Preis-/Leistungsverhältnis an, zum zweiten gehen Mitarbeiter/innen in den wohlverdienten Ruhestand die diese Aufgabe über viele Jahre hinweg ausgeführt haben. Das Schließen dieser personellen Lücken geht mit hohen Ausbildungskosten einher. Zudem nehmen die Anforderungen gerade im Hinblick auf die **MaRisk AT 9** zu, deren Einhaltung und Umsetzung gerade für kleinere Kreditinstitute immer höhere Anstrengungen erfordert. Anfang 2014 durch zwei Unternehmensberatungen durchgeführte Befragungen in der S-Finanzgruppe als auch bei Genossenschaftsbanken belegen die Sorgen der Kreditinstitute, dass die Umsetzung der bankfachlichen Anforderungen wie zum Beispiel der MaRisk als eine der größten Herausforderungen angesehen werden, neben dem Problem der heutigen Niedrigzinspolitik der EZB und damit verbunden das Abschmelzen der heutigen Ertragssituation.

Da die Auslagerung nicht zu einer Delegation der **Verantwortung der Geschäftsleitung** an das Auslagerungsunternehmen führen darf und damit die Leitungsaufgaben der Geschäftsleitung nicht auslagerbar sind, ist die Herausforderung eines Kreditinstitutes, die Auslagerung/Outsourcing ganzheitlich zu überwachen.

Somit müssen alle Verträge bewertet werden. Hier lassen sich die **Verträge in drei Kategorien** einteilen. Die Kategorie eins enthält alle Outsourcing Verträge, die weder Bankgeschäfte, Finanzdienstleistungen, sonstige institutsspezifische Dienstleistungen oder allgemeine Service- und Unterstützungsdienstleistungen beinhalten. Zu betrachten sind hier die Sonderfälle „sonstiger Fremdbezug von Leistungen“, heißt einmalig bezogene Leistungen

oder den Bezug von Leistungen von einem beaufsichtigten Unternehmen. Bei der Kategorie zwei handelt es sich um Outsourcing Verträge. Hier erbringt das eigene Institut gegebenenfalls Dienstleistungen für Dritte, zum Beispiel DV-Dienstleistungen oder Leistungen des eigenen Datenschutzbeauftragten oder Informationssicherheitsbeauftragten für das Nachbarinstitut.

In die Kategorie drei fallen alle klassischen Outsourcing Verträge. Um zu ermitteln, ob ein Outsourcing Vertrag vorliegt oder es sich um einen Vertrag der Kategorie eins oder zwei handelt, wird eine **Risikoanalyse** vorgenommen. Diese Risikoanalyse bewertet die Leistungsrisiken des Dienstleisters anhand der Parameter Marktstellung, Erfahrung, Image, finanzielle und personelle Ressourcen, Sach- und IT-Ausstattung, Funktionsfähigkeit der internen Revision, etc. Zusätzlich werden weitere Anbieter betrachtet. Der zweite Block der Risikoanalyse stellt die Bewertung der strategischen Risiken dar. Hierbei geht es darum, die eigene Einschränkung der Handlungsfähigkeit als auch der Verlust des eigenen Know-Hows festzuhalten und damit die mögliche Abhängigkeit zum Dienstleister herauszuarbeiten. Das Ergebnis der Risikoanalyse stellt die Risikoeinschätzung dar, das heißt: handelt es sich um eine **wesentliche** oder **unwesentliche** Auslagerung. Abhängig von diesem Ergebnis ist die Überwachung der Auslagerung. Verschiedene Verbände haben zum Thema Risikoanalyse ihren angeschlossenen Instituten Muster zur Verfügung gestellt. Es sollte jedoch möglich sein, das ein Institut individuelle Anpassungen der Risikoanalyse Parameter vornehmen kann.

Zur Überwachung der wesentlichen als auch unwesentlichen Verträge sollte das Kreditinstitut verschiedene Informationen einem Outsourcing Vertrag anheften. Neben den Stammdaten sollten unbedingt Daten wie Kündigungstermine, Kosten, Zuständigkeiten und Pflichten von internen und externen Personen (z.B. Meldepflicht an die BaFin), aufsichtsrechtliche Anforderungen, Datenschutz-Regelungen sowie Service Level Vereinbarungen hinterlegt werden. Da die **Service Level Parameter** pro Dienstleister sehr individuell sind, müssen diese per Freitext zuerst erfasst und in einem zweiten Schritt über die Zuordnung von harten Vergleichskriterien messbar gemacht werden (Erfüllungsgrad, Prozentangabe, Schulnoten, etc.). Über einen Beurteilungsbogen sollten alle Dienstleister jährlich bewertet werden. Parameter hierzu wären die Einhaltung der Service Level, Veränderung der Risikosituation. Das Ergebnis kann dann dem Vorstand anhand einer Ampel Funktion (Rot, gelb, grün) präsentiert werden. Zudem sollte jede größere **Vertragsverletzung** protokolliert werden, heißt Beginn und Ende der Beeinträchtigung, Auswirkungen für die Fachabteilungen, etc. Diese Vertragsverletzungen bilden dann die Agenda der jährlich mit dem Dienstleister gerade von wesentlichen Outsourcing Verträgen stattfindenden Servicegesprächen, die ebenfalls dem Outsourcing Vertrag angehängen werden.

Die wichtigste Funktion zur Überwachung von wesentlichen Outsourcing Verträgen ist die **jährliche Prüfung des Revisionsberichtes des Dienstleisters**, der dem Institut zur Verfügung gestellt werden muss. Hier wird die Funktionsfähigkeit der Revision des Dienstleisters überprüft. Wichtig ist hierbei die Abgrenzung des Revisionsberichtes des Dienstleisters von der Risikotragfähigkeit (Risikoanalyse).

Die Überwachung von Outsourcing muss als ganzheitliches Thema betrachtet werden. Somit benötigt ein Kreditinstitut verschiedene Prozesse wie zum Beispiel

- Sondierung einer Auslagerung
- Umsetzung einer Auslagerung
- Jährliche Überwachung
- Dokumentation von Vertragsverletzungen

- Rücknahme einer Auslagerung

an dem verschiedenste Personen bzw. Abteilungen wie Fachabteilung, Organisation, IT, Revision, Datenschutzbeauftragter, Rechtsabteilung, Informationssicherheitsbeauftragten, etc. aktiv eingebunden werden müssen.

Gerade der letztgenannte Prozess bekommt im Hinblick auf die **Neuerung der MaRisk AT 9 Tz. 5** einen größeren Stellenwert. Hier muss das Institut bei wesentlichen Auslagerungen dokumentieren, welche Vorkehrungen unternommen wurden, um die Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse auch nach Beendigung zu gewährleisten.

Der Autor hat mit verschiedenen Kreditinstituten wie Sparkassen und Volksbanken und einer der drei größten Unternehmensberatungen eine Software Lösung zur Abbildung und Überwachung von Outsourcing Verträgen auf Basis der Anforderungen der MaRisk entwickelt.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminartipps zum Thema:

[Dienstleistermanagement, 10. November 2014, Berlin](#)

[Prüfung Dienstleistermanagement, 11. November 2014, Berlin](#)

Weitere interessante Veranstaltungen:

[Herausforderung IT – Strategie, 14. Mai 2014, Frankfurt/M.](#)

[IT-Dokumentation: schlank und revisionssicher, 15. Mai 2014 in Frankfurt/M.](#)

[Sicherheitsrisiko Mobile Endgeräte, 26. Mai 2014, Düsseldorf](#)

[Reputationsrisiko Social Media, 27. Mai 2014, Düsseldorf](#)

[Vergabe und Kontrolle von IT-Berechtigungen, 25. Juni 2014 in Frankfurt/M.](#)

[2. Fachtagung IT-Sicherheit, 26.-27. Juni in Frankfurt/M.](#)

[Wirksame Notfallprozesse und Wiederanlaufplanung, 12. November 2014, Berlin](#)

Hier können Sie unseren aktuellen [Seminarkatalog](#) für 2014 herunterladen.

Aktuelle Buchneuerscheinung

[Bearbeitungs- und Prüfungsleitfaden Datenschutz & IT-Sicherheit 3. Auflage](#)

Die technisch-organisatorischen Maßnahmen des Datenschutzes und der IT-Sicherheit in Kreditinstituten sind geprägt von zunehmenden gesetzlichen und regulatorischen Anforderungen. Des Weiteren stellt die hohe Sensibilität der Kunden bei Datenschutzverstößen und technischen Problemen ein erhebliches Reputationsrisiko für die Bank dar. Diesbezüglich stehen insbesondere die betrieblichen Datenschutz- und IT-Sicherheitsbeauftragten vor großen Herausforderungen. [weiter lesen](#)

Datenschutzrisiken bei Facebook-Fanpages von Banken

Banken können sich ihren Kunden auf Facebook mittels Fanpages präsentieren. Viele rechtliche Fragen zu diesen Fanpages sind nicht abschließend geklärt. Das liegt zum einen daran, dass 16 Landes- und 1 Bundesbehörde für die Datenschutzaufsicht zuständig sind: Häufig vertreten diese Behörden keine einheitlichen Standpunkte.

Zum anderen gibt es nur **wenig Rechtsprechung**, die sich mit datenschutzrechtlichen Fragen bei Fanpages befasst. Das dürfte auch darin begründet sein, dass viele Unternehmen eine rechtliche Auseinandersetzung mit den Aufsichtsbehörden scheuen.

In jüngster Zeit wurden jedoch mehrere rechtliche Auseinandersetzungen mit dem unabhängigen **Landeszentrum für Datenschutz Schleswig-Holstein** (ULD) vor dem Verwaltungsgericht Schleswig-Holstein geführt.¹ Es überrascht wenig, dass diese Rechtsstreite gerade mit dem ULD geführt wurden. Es dürfte einhelliger Auffassung entsprechen, dass das ULD bundesweit die strengsten Vorgaben zum Datenschutz aufstellt.

Insoweit kann man auch von einem Nord-Süd-Gefälle sprechen: Südliche Behörden wie der bayerische Landesbeauftragte für den Datenschutz neigen bei der rechtlichen Bewertung von Datenschutzfragen eher zu einer liberalen Haltung.

In den entschiedenen Fällen ging es immer um dasselbe rechtliche Problem²: Das ULD vertritt die Auffassung, dass „die von Facebook vorgenommene Datenverarbeitung generell **nicht mit deutschem Datenschutzrecht vereinbar** ist, u. a. weil die Nutzung von Fanpages personenbezogen erfasst wird, gegen die Profilbildung keine Widerspruchsmöglichkeit eingeräumt wird, beim Setzen von Cookies keine wirksamen Einwilligungen eingeholt werden und weil für die Betroffenen nicht die geforderte Transparenz hergestellt wird“.

Zur Gewährleistung der Einhaltung des BDSG und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen, § 38 Abs. 5 S. 1 BDSG. Das ULD hat gegen die Betreiber von Fanpages (was im Zweifel auch Banken sein könnten) eine Unterlassungsverfügung gem. § 38 Abs. 5 BDSG erlassen.³ Gegen diese Unterlassungsverfügungen haben sich drei Unternehmen mit Widerspruch und Anfechtungsklage zur Wehr gesetzt.

Das Schleswig-Holsteinische Verwaltungsgericht hat auf die drei Klagen hin in der ersten Instanz am 9. Oktober 2013 entschieden, dass **deutsche Betreiber von Facebook-**

1 Az. 8 A 37/12, 8 A 14/12, 8 A 218/11.

2 Die nachfolgende Darstellung orientiert sich an der Schilderung durch das ULD, vgl. hierzu <https://www.datenschutzzentrum.de/presse/20131010-facebook-vg-urteil.htm> und <https://www.datenschutzzentrum.de/presse/20131101-berufung-fanpages.htm> (zuletzt abgerufen am 6.1.14).

3 Ein Beispiel für eine entsprechende Unterlassungsverfügung findet sich im Internet: <https://www.datenschutzzentrum.de/facebook/20111104-facebook-anordnung-fanpage.html> (zuletzt abgerufen am 6.1.14).

Fanpages für die bei Facebook erfolgende Datenverarbeitung datenschutzrechtlich nicht verantwortlich sind.⁴

In der Urteilsbegründung wurde dargelegt, Fanpagebetreiber könnten für den genutzten Dienst datenschutzrechtlich nicht verantwortlich gemacht werden, weil sie auf das Angebot von Facebook keinen direkten Einfluss nehmen könnten und auch keinen Zugriff auf die personenbezogenen Daten hätten. Dass dies faktisch zu einer Beschränkung des Datenschutzes führe, müsse angesichts der gesetzlichen Regelung hingenommen werden. Wegen der grundsätzlichen Bedeutung der Urteile ließ das VG Schleswig Holstein die Berufung zu.

Das ULD hat gegen eines der Urteile des VG Schleswig-Holstein vom 09.10.2013 Berufung eingelegt. Über die Berufung war bei Redaktionsschluss noch nicht entschieden. Es bleibt abzuwarten, ob die unternehmensfreundliche Rechtsauffassung des VG Schleswig-Holstein bestätigt wird. Insoweit besteht auch für Unternehmen in Schleswig-Holstein noch keine Rechtssicherheit.

Selbst wenn die Entscheidung des VG Schleswig-Holstein bestätigt werden sollte, verbleiben für die Praxis **Anwendungsfragen**. Dies nicht zuletzt vor dem Hintergrund, dass die Entscheidung des Oberverwaltungsgerichts Schleswig-Holstein für die Gerichte der anderen Bundesländer nicht verbindlich wäre.

Es ist also denkbar, dass z.B. das Oberverwaltungsgericht Hamburg die datenschutzrechtliche Verantwortung von Fanpagebetreibern bejaht. Hieran zeigt sich, dass der Förderalismus bei der Findung von einheitlichen Rechtsgrundsätzen für den Datenschutz nicht förderlich ist.

Darüber hinaus ist zu berücksichtigen, dass das soziale Netzwerk Facebook einen permanenten Wandel unterliegt und **ständig neue Rechtsprobleme** entstehen. Demgegenüber ist noch verhältnismäßig wenig Literatur zu den datenschutzrechtlichen Fragen im Zusammenhang mit Facebook veröffentlicht worden. Daran wird auch die Entscheidung des Oberverwaltungsgerichts Schleswig Holstein nichts ändern. Diese stellt nur ein einzelnes Urteil dar, das zumindest nicht deutschlandweit verbindlich ist und nur einen einzelnen Rechtsstreit entscheidet.

Banken wollen Ihre Fanpage trotzdem rechtssicher gestalten. Dies ist aufgrund der aufgezeigten Probleme schwierig. Ein gangbarer Weg dürfte darin bestehen, Fragen zum Thema Facebook und Datenschutz mit der jeweils zuständigen **Aufsichtsbehörde abzustimmen**.

Dr. Ulrich Hallermann, Rechtsanwalt, Investitions- und Strukturbank Rheinland-Pfalz (ISB)

Seminar- und Buchtipps zum Thema

[Seminar Reputationsrisiko Social Media, 27. Mai 2014, Düsseldorf](#)

[Bearbeitungs- und Prüfungsleitfaden Social Media für Banken und Sparkassen](#)

⁴ Der anonymisierte Abdruck einer der inhaltlich gleichlautenden Urteile vom 09.10.2013 ist im Internet zu finden unter <https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf> (zuletzt abgerufen am 6.1.14).

Neuer Buchkatalog

Hier können Sie unseren neu erschienenen [Buchkatalog](#) für das 1. Hj 2014 herunterladen.

Checklisten-Download und Banken-Times Archiv online

Für alle Bücher aus der Reihe unserer „**Bearbeitungs- und Prüfungsleitfäden**“ stellen wir die enthaltenen Checklisten auf unserer Webseite unter „[Mein FCH](#)“ als veränderbare WORD-Datei zum Download zur Verfügung. Den Zugangscode finden Sie im Buch.

Zusätzlich stehen im Bereich „Mein FCH“ auch alle erschienenen **Banken-Times** und Banken-Times SPEZIAL Ausgaben als PDF zum Download bereit.

Impressum

Finanz Colloquium Heidelberg GmbH – Plöck 32a – 69117 Heidelberg

VisdP: Thomas Göhrig

Telefon: 0 62 21 / 99 89 8-0 - Telefax: 0 62 21 / 99 89 8-99

E-Mail: Info@FC-Heidelberg.de – Internet: www.FC-Heidelberg.de

Geschäftsführer:

Dr. Christian Göbes, Frank Sator, Dr. Patrick Rösler, Marcus Michel, Michael Helfer, Thomas Göhrig

Sitz der Gesellschaft ist Heidelberg, Amtsgericht Mannheim, HRB Nr. 335598

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de.